REMARKS

Applicants appreciate the courtesy extended by Examiner Okoronkwo in conducting a telephone interview with Applicants' representative on December 18, 2007. During the interview, Applicants' representative explained how the Applicants' claimed invention distinguishes over the prior art, in particular, the Douglas and Maier references. Also discussed was an amendment to the independent claims to clarify that the claimed "IDS log analysis support apparatus" is arranged separately from an intrusion detection system (IDS). As amended, independent claims 1, 11, and 21 incorporate this limitation.

Claims 1-30 are pending in the application. Independent claims 1, 11, and 21 have been amended to recite that the support apparatus is arranged separately from an intrusion detection system (IDS). The amendments are fully supported by the application as originally filed (see, e.g., specification at page 16, lines 15-19; and FIG. 1).

Claims 1-30 were rejected under 35 USC 103(a) as being unpatentable over U.S. Patent 7,152,242 to Douglas in view of U.S. Patent 5,625,815 to Maier et al. ("Maier"). This rejection is respectfully traversed.

Regarding the rejection of independent claims 1, 11, and 21 over the proposed combination of Douglas in view of Maier, the Douglas and Maier references, whether taken alone or in combination, do not teach or suggest a support apparatus, method, and program in which logs of an intrusion detection system ("IDS") are regularly collected, the logs are managed and stored in a database, and statistics are obtained for the logs managed by the database in order to perform analysis of the statistics, where the support apparatus is arranged separately from the intrusion detection system.

On page 3, last paragraph of the Office Action of 10/01/2007, column 2, lines 17-20 and 29-35 of Douglas were cited allegedly for teaching the Applicants' claimed "log collection section" and "log analysis section" recited in independent claim 1 (and related limitations of independent claims 11 and 21).

Referring to column 2, lines 14-36 of Douglas, the invention of Douglas "forms one tool of an intrusion detection system (IDS)" (see column 2, lines 14-15), and includes a host-based IDS sensor 20 that "detects attacks targeted at the host system on which it is installed" (see column 2, lines 31-33). As stated in column 2, lines 35-36: "the HIDS sensor 20 detects attacks by monitoring the output to the system and audit logs."

In other words, Douglas discloses various components of an intrusion detection system (IDS), where the detection capabilities disclosed in Douglas are performed within the IDS.

There is no teaching or suggestion of the Applicants' claimed IDS log analysis support apparatus arranged separately from the intrusion detection system, where the support apparatus collects logs of an intrusion detection system. In Douglas, any collection functions are performed internally within the intrusion detection system.

Further, there is simply no teaching or suggestion in Douglas of the claimed analysis of statistics of logs managed by a database. In Douglas, the monitoring of system output and audit logs performed within the IDS is not equivalent to the claimed "log analysis section" that obtains statistics and performs statistical analysis based on logs stored in a database.

The Maier reference was cited allegedly for teaching a database (see page 4 of Office Action of 10/01/2007).

In Maier, a database is disclosed in which the structure of a database table or index can be altered "while the database table or index remains available for execution of transactions" (see column 2, lines 39-43 of Maier).

However, Maier does not teach or suggest a database that "stores and manages logs collected by the log collection section" (independent claim 1; *see also* independent claims 11 and 21).

Moreover, Maier is not related to a log analysis support apparatus, method, or program, and is not even directed to an intrusion detection system. In Maier, the database is structured to allow continued availability for transaction execution even while the database is being altered, which is not relevant to the Applicants' claimed invention in which a database must store and manage logs collected by a log collection section.

For at least the reasons discussed above, the proposed combination of Douglas in view of Maier does not teach or suggest the Applicants' claimed invention. Therefore, independent claims 1, 11, and 21 and their respective dependent claims are patentable over the proposed combination.

It is believed the application is in condition for immediate allowance, which action is earnestly solicited.

Respectfully submitted,

/Steven M. Jensen/

Date: January 16, 2008

Steven M. Jensen
(Reg. No. 42,693)
Edwards Angell Palmer & Dodge
P.O. Box 55874
Boston, MA 02205

Phone: (617) 239-0100

Customer No. 21874